ABSTRACT

The inventive subject matter provides reliable methods and apparatus for secure communication within a network collaboration group including a VPN. Distribution of critical group data to member nodes (such as encryption keys for communication with other member nodes) is preferably handled by master nodes in a manner relatively resistant to misbehavior by current, past, or other nodes, and to outsider attacks such as replay attacks. A particular embodiment enables distribution of critical group data by master nodes to member nodes in a manner that offers confidentiality (the critical data cannot be read by eavesdropper), integrity (the receiving member node has evidence that the critical data has not been tampered with in transit), authenticity (the receiving member node has evidence that the critical data was sent by a master node), and freshness (the critical data is not a replay of a previous message). In an embodiment, communication of critical data between the master node and the member node may be encrypted with a session key. Preferably, in each round of communication between master and member, the transmitting node generates a new nonce value and embeds it in the encrypted communication, for use by the recipient in the next communication. This nonce value typically becomes the expected nonce, for purposes of the next communication. If the next communication does not contain the expected nonce value, then the communication may be readily identified and rejected by the recipient as a replay attack or otherwise illicit communication.